UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/630,069	07/31/2000	Christopher L. Hamlin	K35A0638	5762

26332 7590 09/28/2005

WESTERN DIGITAL CORP.
20511 LAKE FOREST DRIVE
C205 - INTELLECTUAL PROPERTY DEPARTMENT
LAKE FOREST, CA 92630

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/630,069	HAMLIN, CHRISTOPHER L.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *29 June 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 29 June 2005, the original application was filed on 31 July 2000.

2. Claims 1-26 are currently pending in this application. Claims 1, 12, and 22 are independent claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-5, 7, 9, 11-17, 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Alonso et al. U.S. Patent No. 6,434,700 (hereinafter '700) in further view of Jackson, Trevor European Patent Application No. 0911738 (hereinafter '738).

As to independent claim 1, "A computer network comprising a plurality of interconnected network devices including: (a) a plurality of client computers; (b) an authentication server computer operated by a system administrator; and (c) a disk drive connected to the authentication server computer; the disk drive comprising: an interface for receiving personal authentication data and user access data from the system administrator" is taught in '700 col. 5, line 62 through col. 6, line 29 "Upon receiving the request, the network access server sends the user access information to a centralized server,

such as an Access Control Server ("ACS") ... The ACS determines who may access the network what services they are authorized to use, and to whom the provides Authorization, Authentication, and Accounting ("AAA") functions for a managed network ... Each of the network devices can be configured to communicate with the ACS";

"a disk for storing data" is shown in '700 col. 2, lines 6-7 and col. 6, lines 16-19 "Generally, a Fortezza security system includes a Fortezza Crypto card that stores unique encrypted information" and "The ACS integrates and supports various authentication and authorization technologies, including token cards, and Fortezza security systems";

the following is not taught in '700:

"a disk controller for controlling access to the disk; an authenticator, responsive to the personal authentication data, for enabling the disk controller" however '738 teaches "Accordingly, the present invention provides an improved disk drive having: at least one hard disk; drive control means for controlling operation of the drive; and read/write means for reading data from, and writing data onto, said at least one hard disk; wherein the improvement comprises the provision of encryption/decryption means, connected to said read/write means, for encrypting data to be written onto, and decrypting data to be read from, said at least one hard disk; said drive control means including permanent security control means formed and arranged for restricting read/write access to said at least one hard disk via said encryption/decryption means, for at least the data content of data files to be written thereto or read therefrom, and password-dependent security control means formed and arranged for receiving user input password data, comparing said user input password data with predetermined password data stored in said password-dependent security control means, and for

activation of said encryption/decryption means only in response to receipt of a valid password, whereby read/write access to said at least one hard disk, in relation to at least the data content of data files, is restricted to holders of a valid password" in col. 2, lines 17-39;

"cryptographic circuitry for encrypting the user access data received from the system administrator into encrypted data stored on the disk" however '738 teaches "Preferably, the encryption/decryption means is provided in integrated circuitry in the disk drive" in col. 2, lines 47-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify an authorization access server taught in '700 to include an improved disk drive. One of ordinary skill in the art would have been motivated to perform such a modification because their exists a need for protecting data stored on computer systems see '738 (col. 1, lines 9 et seq.) "The need for protecting data stored on computer systems is a wide-ranging issue. Computer hackers, destruction of data by viruses, loss of computer equipment and the theft of data are commonplace. The nature of data stored in computer files can be such that its loss or disclosure can be financially, politically or personally damaging. Consequently there have been many data protection systems proposed which address these issues, many of these involving some form of data encryption".

As to dependent claim 2, "wherein the user access data comprises a plurality of user identifiers and corresponding access rights to the plurality of network devices" is disclosed in '700 col. 6, lines 16-29.

As to dependent claim 3, "The computer network as recited in claim 2, wherein the user access data further comprises user authentication data" is shown in '700 col. 6, lines 16-29.

As to dependent claim 4, "The computer network as recited in claim 3, wherein the user authentication data comprises a user password" is taught in '738 col. 2, lines 17-39.

As to dependent claim 5, this claim contains texts that contain substantially similar limitations as cited in claim 4 and are rejected along the same rationale.

As to dependent claim 7, "The computer network as recited in claim 2, wherein: (a) the disk stores encrypted device access data associated with the network devices; and (b) the device access data for use in authenticating device access requests transmitted from client computers to the network devices" is taught in '700 col. 8 line 55 – col. 9 line 23 "FIG. 3 is a flow diagram of one embodiment of a method for allowing users of Fortezza passwords to use computer networks supporting a variety of authentication and authorization technologies. FIG. 3 will be explained with reference to the components in FIG. 2. However, the method of FIG. 3 may be implemented with any other arrangement of hardware and software elements that may carry out the functions needed in the method of FIG. 3. Thus, the method of FIG. 3 is not intended to be limited to the context of FIG. 2. At block 300 of FIG. 3, client 102 establishes a connection 116 with the network access server 104. For example, user 106 associated with client 102 causes the client 102 to dial in and send user access information to the network access server 104. The user access information typically contains a username and password. The password can be a fixed password or an OTP type password obtained through the use of a Smart card or Token card, depending on the level of authentication. The password type can also be a Fortezza

password which is a unique hash value produced by a Fortezza Crypto card 107a and Fortezza card reader 107b. The more authorization privileges a user receives, the stronger the authentication would be. At block 302, the network access server 104 receives user access information from client 102. In system 200, the communications function of accessing the network, and the structure that supports this function, are separated from the security functions and the structure that carries them out. Hence, at block 304, the network access server 104 passes the user access information to the Access Control Server 202. The network access server 104 controls modems and ports that are used to connect to network 108, but does not examine the type of password contained in the user access information. It simply forwards the user access information to the Access Control Server 202 which is a point of centralized control of network access and the provision security services".

As to dependent claim 9, "The computer network as recited in claim 7, wherein: (a) the interface receives unencrypted device access data; and (b) the cryptographic circuitry encrypts the unencrypted device access data into the encrypted device access data stored on the disk" is disclosed in '738 col. 4, lines 7-18 ". Advantageously, the permanent security control means is adapted to restrict read/write access to the disk or disks by causing all data to be written to, and all data to be read from, the disk(s) to be routed through the encryption/decryption means. Alternatively the permanent security control means may only cause some data to be routed through the encryption/decryption means, for example only the data content of data files and not the address content of said data files. In its activated state, the encryption/decryption means advantageously encrypts all data routed there through from the permanent security control means. The encrypted data from the encryption/decryption means is

then written onto the disk(s) via the read/write means. The activated encryption/decryption means also decrypts all encrypted data read from said disk(s) by the read write means"

As to dependent claim 11, "The computer network as recited in claim 7, wherein the encrypted device access data is transmitted from the network devices to the disk drive" is taught in '738 col. 4, lines 7-18.

As to independent claim 12, "A computer network comprising a plurality of interconnected network devices including: (a) a plurality of client computers; (b) an authentication server computer; and (c) a disk drive connected to the authentication server computer, the disk drive comprising: an interface for receiving from a client computer a user ID and a user access request to access a network device, and for transmitting device access data to the client computer" and **"wherein the disk controller uses the decrypted data to generate the device access data transmitted to the client computer"** is taught in '700 col. 5, line 62 – col. 6, line 29;

"a disk for storing encrypted data, a disk controller" is shown in '700 col. 2, lines 6-7 and col. 6, lines 16-19;

the following is not taught in '700:

"responsive to the user ID and user access request, for controlling access to the disk; and cryptographic circuitry for decrypting the encrypted data stored on the disk to generate decrypted data" however '738 "Accordingly, the present invention provides an improved disk drive having: at least one hard disk; drive control means for controlling operation of the drive; and read/write means for reading data from, and writing data onto, said at least one hard disk ..." in col. 2, lines 17-39.

As to dependent claim 13, "The computer network as recited in claim 12, wherein: (a) the encrypted data comprises encrypted user authentication data corresponding to the user ID; and (b) the cryptographic circuitry decrypts the encrypted user authentication data to generate decrypted user authentication data" is shown in '738 col. 4, lines 7-18

As to dependent claim 14, "The computer network as recited in claim 13, wherein the decrypted user authentication data comprises a user password" is taught in '738 col. 2, lines 17-39.

As to dependent claim 15, "wherein the cryptographic circuitry encrypts the device access data before transmission to the client computer" is shown in '738 col. 4, lines 7-18.

As to dependent claim 16, "(a) the cryptographic circuitry encrypts the device access data before transmission to the client computer; and (b) the cryptographic circuitry encrypts the device access data using a cryptographic user key extracted from the decrypted user authentication data" is taught in '738 col. 4, lines 43-67 "The discrete security key device may conveniently comprise a portable key card which contains user input password data for inputting to the password-dependent security control means of the drive, via the security key interface device provided as part of the data access security control system. The security key interface device may be provided in the disk drive itself or may, alternatively, be provided in a host computer in which the drive is installed. Thus, said security key interface may comprise a part of, or may alternatively be formed and arranged for electrical connection to, the password-dependent security control means of the drive. The portable key card may include a TROM

(Touch Read Only Memory) for contacting an input/output port of the security key interface device, said TROM containing said user input password data".

As to dependent claim 17, " The computer network as recited in claim 16, wherein the cryptographic user key is generated by the cryptographic circuitry using the decrypted user authentication data" is shown in '738 col. 4, lines 43-67.

6. **Claims 6, 8, 10, and 18-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over '700 and '738 as applied to claims 1 and 12 in further view of DeTreville U.S. Patent No. 6,609,199 (hereinafter '199).

As to dependent claim 6, the following is not taught in '700 and '738 **"wherein: (a) the cryptographic circuitry comprises an immutable secret drive key configured during manufacture of the disk drive; and (b) the secret drive key for use in encrypting the user access data"** however '199 teaches "Computers 102 and 104 include access ports 112 and 114, respectively. Access ports 112 and 114 allow a portable integrated circuit (IC) device, such as device 116, to be communicably coupled to computers 102 and 104 (e.g., device 116 may be inserted into ports 112 and 114). This coupling can be accomplished in any of a variety of conventional manners" and "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU. For discussion purposes, the CPU's public key is referred to as "K.sub.CPU " and the corresponding private key is referred to as "K.sub.CPU.sup.-1 ". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible to arbitrary application or operating system code)" in col. 4 lines 7-9 and col. 5 lines 54-60.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify an authorization access server with a disk drive for controlling access to the contents stored in the drive taught in '700 and '738 to include a secret device key. One of ordinary skill in the art would have been motivated to perform such a modification because secret device key put in place by a manufacturer is well known in the art to maintain security see '199 (col. 2, lines 27 et seq.) "The invention addresses these disadvantages, providing an improved way to maintain the security of private information on a portable IC device".

As to dependent claim 8, "wherein the encrypted device access data comprises an encrypted secret device key shared with a corresponding network device" is taught in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU. For discussion purposes, the CPU's public key is referred to as "K.sub.CPU.sup-1". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible to arbitrary application or operating system code)".

As to dependent claim 10, "wherein the encrypted device access data is stored on the disk during manufacture of the disk drive" is taught in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU. For discussion purposes, the CPU's public key is referred to as "K.sub.CPU.sup-1". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible to arbitrary application or operating system code)".

As to dependent claim 18, "wherein the cryptographic user key is a public key for use in a public key encryption algorithm" is shown in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU".

As to dependent claim 19, "wherein: (a) the cryptographic circuitry encrypts the device access data using a secret device key shared with the network device; and (b) the secret device key is used by the network device to authenticate device access requests received from client computers" is shown in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU".

As to dependent claim 20, "The computer network as recited in claim 19, wherein the secret device key shared with the network device is stored in encrypted form on the disk is shown in '700 col. 2, lines 6-7 and col. 6, lines 16-19 "Generally, a Fortezza security system includes a Fortezza Crypto card that stores unique encrypted information, and which executes encryption algorithms to produce a scrambled one-time password ("OTP"). The card is a self-contained hardware system" and "The ACS integrates and supports various authentication and authorization technologies, including token cards, and Fortezza security systems";

"and decrypted by the cryptography circuitry" is shown in '738 col. 4, lines 19-26.

As to dependent claim 21, "The computer network as recited in claim 12, wherein: (c) the cryptographic circuitry comprises an immutable secret drive key configured during

manufacture of the disk drive; and (d) the secret drive key for use in decrypting the encrypted data stored on the disk" is shown in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU. For discussion purposes, the CPU's public key is referred to as "K.sub.CPU " and the corresponding private key is referred to as "K.sub.CPU.sup.-1". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible" to arbitrary application or operating system code)".

7. **Claims 22-26** are rejected under 35 U.S.C. 103(a) as being unpatentable over '700 and '738 in further view of '199.

As to independent claim 22, "A computer network comprising a plurality of interconnected network devices including: (a) a plurality of client computers; (b) an authentication server; and (c) a disk drive comprising: an interface for receiving an encrypted device access request and for inputting/outputting user data from/to a client computer; a disk for storing data; " is taught in '700 col. 5, line 64 – col. 6, line 29 "the network access server sends the user access information to a centralized server, such as an Access Control Server ("ACS"). The ACS provides a central point of control for the management of multiple security services, and network devices"

"a disk controller for controlling access to the disk; an internal drive key;" and "an authenticator, responsive to the decrypted secret device key, for authenticating the device access request" is shown in '738 col. 2, lines 17-39 "Accordingly, the present invention provides an improved disk drive having: at least one hard disk; drive control means for controlling operation of the drive; and read/write means for reading data from, and writing data

onto, said at least one hard disk; wherein the improvement comprises the provision of encryption/decryption means, connected to said read/write means, for encrypting data to be written onto, and decrypting data to be read from, said at least one hard disk; said drive control means including permanent security control means formed and arranged for restricting read/write access to said at least one hard disk via said encryption/decryption means, for at least the data content of data files to be written thereto or read therefrom, and password-dependent security control means formed and arranged for receiving user input password data";

the following is not taught in '700 and '738:

"a secret device key shared with the authentication server, the secret device key stored in encrypted form; cryptographic circuitry, responsive to the internal drive key, for decrypting the encrypted secret device key to generate a decrypted secret device key"

however '199 teaches "Computers 102 and 104 include access ports 112 and 114, respectively. Access ports 112 and 114 allow a portable integrated circuit (IC) device, such as device 116, to be communicably coupled to computers 102 and 104 (e.g., device 116 may be inserted into ports 112 and 114). This coupling can be accomplished in any of a variety of conventional manners" and "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU. For discussion purposes, the CPU's public key is referred to as "K.sub.CPU " and the corresponding private key is referred to as "K.sub.CPU.sup.-1 ". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible to arbitrary application or operating system code)" in col. 4 lines 7-9 and col. 5 lines 54-60.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify an with a disk drive for controlling access to the contents stored in the drive taught in '700 and '738 to include a secret device key. One of ordinary skill in the art would have been motivated to perform such a modification because secret device key put in place by a manufacturer is well known in the art to maintain security see '199 (col. 2, lines 27 et seq.) "The invention addresses these disadvantages, providing an improved way to maintain the security of private information on a portable IC device".

As to dependent claim 23, "The computer network as recited in claim 22, wherein the encrypted secret device key stored on the disk" is taught in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU. For discussion purposes, the CPU's public key is referred to as "K.sub.CPU " and the corresponding private key is referred to as "K.sub.CPU.sup.-1 ". Other physical implementations may include storing the key on an external device to which the main CPU has privileged access (where the stored secrets are inaccessible to arbitrary application or operating system code)"

As to dependent claim 24, "The computer network as recited in claim 22, wherein the encrypted secret device key is configured during manufacture of the disk drive" is shown in '199 col. 5 lines 54-60 "The CPU manufacturer equips the CPU 134 with a pair of public and private keys 150 that is unique to the CPU.

As to dependent claim 25, "The computer network as recited in claim 22, wherein the disk drive transmits the encrypted secret device key to the authentication server" is taught in '700 col. 9, lines 9-19 "the network access server 104 receives user access information

from client 102. In system 200, the communications function of accessing the network, and the structure that supports this function, are separated from the security functions".

As to dependent claim 26, "The computer network as recited in claim 22, wherein the internal drive key comprises tamper-resistant circuitry" is taught in '199 col. 6, lines 62-64 "Alternatively, the CPU 134 can store the boot log 158 in volatile memory 138 in a cryptographic tamper-resistant container".

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
13 July 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100